Canad. Math. Bull. Vol. **55** (2), 2012 pp. 390–399
http://dx.doi.org/10.4153/CMB-2011-088-3

Automorphisms of Iterated Wreath Product p-Groups

Jeffrey M. Riedl

Abstract. We determine the order of the automorphism group $\mathrm{Aut}(W)$ for each member W of an important family of finite p-groups that may be constructed as iterated regular wreath products of cyclic groups. We use a method based on representation theory.

1 Introduction

We begin by defining an important family of finite groups of prime-power order. Let p be a prime and let e be a positive integer. Let $W_1^e(p)$ denote the cyclic group of order p^e. For each integer $n \geq 2$, we recursively define $W_n^e(p)$ as the regular wreath product group $W_n^e(p) = W_{n-1}^e(p) \wr \mathbb{Z}_p$. Thus, for $n \geq 2$, the group $W_n^e(p)$ is the semidirect product $N \rtimes \mathbb{Z}_p$ where N is the direct product of p copies of $W_{n-1}^e(p)$, and where $\mathbb{Z}_p$, the cyclic group of order p, acts via automorphisms on N by regularly permuting these direct factors.

It is well known that for an arbitrary prime p and positive integer n, the group $W_n^1(p)$ is isomorphic to a Sylow p-subgroup of the symmetric group of degree p^n. The following two results [6, Theorem 1.4, Theorem 1.5] suggest that the three-parameter family of groups $W_n^e(p)$ is worthy of attention.

Theorem 1.1 *Let $q > 1$ be any prime-power and let p be any prime divisor of $q-1$. Let p^e denote the p-part of $q-1$, so that e is a positive integer. Then for every positive integer n, the general linear group $\Gamma = \mathrm{GL}(p^{n-1}, q)$ contains a subgroup P that is isomorphic to $W_n^e(p)$. Furthermore, if $p^e \geq 3$, then P is a Sylow p-subgroup of Γ.*

We mention without proof that in the situation of Theorem 1.1, it is actually true that P is a Sylow p-subgroup of Γ if and only if $p^e \geq 3$. Although Theorem 1.1 is quite well known, we suspect that the following result might be less well known.

Theorem 1.2 *Let G be a finite p-group for some prime p. Let r be any prime such that $r \neq p$, and let F denote the algebraic closure of the field with r elements. Let n be any positive integer. The following conditions are equivalent.*

(i) *G is isomorphic to a subgroup of the general linear group $\mathrm{GL}(p^{n-1}, \mathbb{C})$.*
(ii) *G is isomorphic to a subgroup of the general linear group $\mathrm{GL}(p^{n-1}, F)$.*
(iii) *G is isomorphic to a subgroup of $W_n^e(p)$ for some positive integer e.*

The purpose of this article is to determine the order of the group of automorphisms $\mathrm{Aut}(W)$ of the group $W = W_n^e(p)$ in case $n \geq 2$ and $p^e \geq 3$.

Received by the editors March 20, 2009; revised July 18, 2009.
Published electronically May 13, 2011.
AMS subject classification: **20D45**, 20D15, 20E22.

Before going further, we explain why these automorphism groups may be of interest. In unpublished work we classified up to isomorphism the nonabelian subgroups H of $W_2^e(p)$ for an arbitrary prime p and positive integer e such that $p^e \geq 3$. (Using Theorem 1.2, one can show that this is equivalent to classifying up to isomorphism the finite p-groups having a faithful irreducible ordinary character of degree p.) Let $A = \mathrm{Aut}(W)$ for $W = W_2^e(p)$. In other unpublished work we prove, for every group H of nilpotence class at least 3 appearing in this classification, that $\mathbf{N}_A(H)/\mathbf{C}_A(H)$ is isomorphic to $\mathrm{Aut}(H)$, which says essentially that the full automorphism group $\mathrm{Aut}(H)$ is realized inside the group $\mathrm{Aut}(W)$. This suggests that knowledge of the structure of the group $\mathrm{Aut}(W)$ could, in principle, be translated into knowledge of the structure of $\mathrm{Aut}(H)$ for many subgroups H of W. Knowing the order of $\mathrm{Aut}(W)$ is a natural first step toward gaining some understanding of the structure of the group $\mathrm{Aut}(W)$.

In order to state the main result, we need to define some notations and make some preliminary remarks. Let p be any prime and let e and n be any positive integers such that $n \geq 2$. It is straightforward to calculate that the order of the group $W_n^e(p)$ is $p^{\alpha(n)}$ where $\alpha(n) = 1 + p + \cdots + p^{n-2} + ep^{n-1}$. In Section 3 we determine character-theoretic information about the group $W_n^e(p)$ that is needed for the main result. We prove that every faithful irreducible ordinary character of $W_n^e(p)$ has degree at least p^{n-1}. Let $\mathcal{F}_n$ denote the set consisting of all faithful irreducible ordinary characters of $W_n^e(p)$ that have degree p^{n-1}. We also prove that the cardinality of the set $\mathcal{F}_n$ is $(p-1)p^{\beta(n)}$ where

$$\beta(n) = (p-1)\left[\binom{n}{2} + (e-1)n\right] - (e-1)(p-2) - 1.$$

(Our proof in Section 3 gives an interesting description of the characters belonging to the set $\mathcal{F}_n$.) Our approach to determining $|\mathcal{F}_n|$ is to show that $|\mathcal{F}_2| = (p-1)p^{ep-2}$ and that

$$|\mathcal{F}_n| = |\mathcal{F}_{n-1}| \cdot p^{(p-1)(n+e-2)} \quad \text{for } n > 2.$$

The formula for $\beta(n)$ that appears above is the unique solution of the recurrence

$$\beta(2) = ep - 2, \qquad \beta(n) = \beta(n-1) + (p-1)(n+e-2) \quad \text{for } n > 2.$$

We are now ready to state the main result.

Theorem A *Let p be a prime and let e and n be positive integers such that $n \geq 2$ and $p^e \geq 3$. For $W = W_n^e(p)$, the automorphism group $\mathrm{Aut}(W)$ has order $(p-1)^n p^r$ where $r = \alpha(n) + \beta(n) - e$.*

We use the automorphism counting formula that was developed in [6] to establish Theorem A. This is a general formula for the order of the automorphism group $\mathrm{Aut}(G)$ of a monolithic finite group G in terms of information about the faithful irreducible ordinary characters of G of minimal degree and information about how G is embedded as a subgroup of a particular finite general linear group. (A finite group is said to be *monolithic* if it has a unique minimal normal subgroup. Thus a finite

https://doi.org/10.4153/CMB-2011-088-3 Published online by Cambridge University Press

p-group is monolithic if and only if the center of the group is cyclic.) We mention that Lentoudis [4,5] determined the order of $\mathrm{Aut}(W)$ for the special case $W = W_n^1(p)$ for odd primes p, using methods completely different from those of this article. The proof of Theorem A appears in Section 2. The character-theoretic results that are used in the proof of Theorem A appear in Section 3.

Let $\mathrm{Irr}(G)$ denote the set of irreducible ordinary characters of a finite group G.

2 The Proof of Theorem A

For each finite group G and each prime-power q, we define $\mathrm{mindeg}(G, q)$ to be the smallest positive integer m such that the general linear group $\mathrm{GL}(m, q)$ contains a subgroup that is isomorphic to G. Thus $\mathrm{mindeg}(G, q)$ is the minimal degree among all the faithful F-representations of the group G, where F denotes the field with q elements.

Definition 2.1 Let G be a monolithic finite group, let q be a prime-power that is relatively prime to the order of G, and let $m = \mathrm{mindeg}(G, q)$. We say that the ordered triple (G, q, m) is a *monolithic triple* in case every faithful irreducible ordinary character of G has degree at least m. Assuming that (G, q, m) is a monolithic triple, we define $\mathcal{F}(G, q)$ to be the set of all faithful irreducible ordinary characters of G of degree m. We say that the monolithic triple (G, q, m) is *good* provided that every value of each character belonging to the set $\mathcal{F}(G, q)$ is a $\mathbb{Z}$-linear combination of complex $(q-1)$-th roots of unity.

The following is a special case of a result that was proved in [6]. We refer to this result as the automorphism counting formula. It is the key to establishing Theorem A.

Theorem 2.2 *Let (G, q, m) be a good monolithic triple. Suppose that $\Gamma = \mathrm{GL}(m, q)$ has a unique conjugacy class of subgroups whose members are isomorphic to G. Let H be any subgroup of Γ that is isomorphic to G. Then $|\mathrm{Aut}(G)|(q-1) = |\mathcal{F}(G, q)| \cdot |\mathbf{N}_\Gamma(H)|$.*

To establish Theorem A, the idea is to define a good monolithic triple (G, q, m) with $G = W_n^e(p)$ that satisfies the hypothesis of Theorem 2.2. The conclusion of Theorem 2.2 would then yield $|\mathrm{Aut}(G)|$ provided that we know in advance $|\mathcal{F}(G, q)|$ and $|\mathbf{N}_\Gamma(H)|$. The next several results will be used to calculate $|\mathcal{F}(G, q)|$ and $|\mathbf{N}_\Gamma(H)|$ in this situation.

The following character-theoretic result will be proved Section 3.

Theorem 2.3 *Let p be a prime. Let e and n be positive integers. Write $W = W_n^e(p)$. We define the set $\mathcal{F} = \{\chi \in \mathrm{Irr}(W) \mid \chi(1) = p^{n-1}$ and χ is faithful$\}$. The following hold.*

(i) *The center of the group W is cyclic of order p^e.*
(ii) *Every faithful irreducible ordinary character of W has degree at least p^{n-1}.*
(iii) *Every value of each character belonging to the set $\mathcal{F}$ is a $\mathbb{Z}$-linear combination of complex p^e-th roots of unity.*
(iv) *If $n \geq 2$, then $|\mathcal{F}| = (p-1)p^{\beta(n)}$, where $\beta(n)$ is as defined in the introduction.*

The following result is included in [6, Theorem 4.4].

https://doi.org/10.4153/CMB-2011-088-3 Published online by Cambridge University Press

Theorem 2.4 *Let $\Gamma = \mathrm{GL}(m,q)$, where $q > 1$ is any prime-power and m is any positive integer. Let F be the field with q elements, let F_0 be any nontrivial subgroup of the multiplicative group $F^\times = F - \{0\}$, and let E be the group of all diagonal matrices in Γ having the property that each entry along the diagonal belongs to F_0. Let S be the subgroup of Γ consisting of all permutation matrices, and note that $S \cong \mathrm{Sym}(m)$. Let T be any transitive subgroup of the symmetric group S and let $H = E \rtimes T$. If E is a characteristic subgroup of H, then*

$$|\mathbf{N}_\Gamma(H)| = |\mathbf{N}_S(T){:}T| \cdot |H|\,(q-1)\,/\,|F_0|.$$

In the situation and notation of Theorem 2.4, the conclusion of that result reduces the problem of calculating the order of $\mathbf{N}_\Gamma(H)$ to the problem of calculating the index $|\mathbf{N}_S(T){:}T|$. The following result, which appears in [1], will be used to calculate the index $|\mathbf{N}_S(T){:}T|$ for the particular situation that arises in the proof of Theorem A.

Theorem 2.5 *Let p be any prime and let n be any positive integer. Let P be any Sylow p-subgroup of the symmetric group $S = \mathrm{Sym}(p^n)$. Then $|\mathbf{N}_S(P){:}P| = (p-1)^n$.*

Recall that in case $n \geq 2$, we recursively defined $W_n^e(p)$ as the semidirect product $N \rtimes \mathbb{Z}_p$, where N is the direct product of p copies of $W_{n-1}^e(p)$. We now describe another useful way to regard $W_n^e(p)$ as a semidirect product. First note that for $n \geq 2$, the fact that $W_{n-1}^1(p)$ is isomorphic to a Sylow p-subgroup of the symmetric group of degree p^{n-1} provides us with a transitive action of $W_{n-1}^1(p)$ on a set of size p^{n-1}. For each positive integer n, the group $W_n^e(p)$ is isomorphic to the semidirect product $B \rtimes T$, where B is the direct product of p^{n-1} copies of the cyclic group of order p^e and where the group T and its action on B are defined as follows. In case $n = 1$, the group T is trivial and thus its action on B is trivial. In case $n \geq 2$, the group T is isomorphic to $W_{n-1}^1(p)$ and acts via automorphisms on B by transitively permuting the p^{n-1} direct factors of B in a manner described earlier in this paragraph.

In the proof of Theorem A, we apply Theorem 2.4 with the groups $W_n^e(p)$ and B playing the roles of H and E in the notation of Theorem 2.4. One hypothesis of Theorem 2.4 is that E is a characteristic subgroup of H, and so we need the following result. This result is a generalization of [2, Satz III.15.4(a)] with the same proof, which we omit here.

Theorem 2.6 *Let p be a prime, let e and n be positive integers, and write $W_n^e(p) = B \rtimes T$, where B and T are as defined earlier. If $p^e \geq 3$, then B is the product of all the abelian normal subgroups of $W_n^e(p)$, and so B is a characteristic subgroup of $W_n^e(p)$.*

In the proof of Theorem A, we use the following result to define an embedding of $W_n^e(p)$ as a subgroup of a general linear group that satisfies the hypotheses of Theorem 2.4

Lemma 2.7 *Let p be a prime, let e and n be positive integers, and write $W_n^e(p) = B \rtimes T$, where B and T are as defined earlier. Let F be any field containing a primitive p^e-th root of unity. Then there exists a faithful F-representation $\mathcal{Y}$ of $W_n^e(p)$ of degree p^{n-1} such that $\mathcal{Y}(B)$ is the group of all diagonal matrices of order dividing p^e in the general linear group $\mathrm{GL}(p^{n-1}, F)$, while $\mathcal{Y}(T)$ is a transitive group of permutation matrices.*

Proof We proceed via induction on n. The base case $n = 1$ is trivial. Let $n > 1$ and assume inductively that $\mathcal{X}$ is a faithful F-representation of $W^e_{n-1}(p)$ of degree p^{n-2} having the desired properties. By definition we have $W^e_n(p) = N \rtimes \langle w \rangle$, where N is the direct product of p copies of the group $W^e_{n-1}(p)$ and the automorphism $w \in \mathrm{Aut}(N)$ cyclically permutes these p direct factors. We now define the homomorphism $\mathcal{Y}\colon W^e_n(p) \to \mathrm{GL}(p^{n-1}, F)$ as follows. For each element $x = (x_1, \dots, x_p) \in N$, we let

$$\mathcal{Y}(x) = \begin{pmatrix} \mathcal{X}(x_1) & 0 & \cdots & 0 \\ 0 & \mathcal{X}(x_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathcal{X}(x_p) \end{pmatrix}.$$

Furthermore, letting I denote the p^{n-2}-by-p^{n-2} identity matrix, we define

$$\mathcal{Y}(w) = \begin{pmatrix} 0 & 0 & 0 & 0 & I \\ I & 0 & \cdots & 0 & 0 \\ 0 & I & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 \\ 0 & 0 & \cdots & I & 0 \end{pmatrix}.$$

The proof is complete. ∎

The following result (which appeared as Lemma 3.2 in [6]) describes the orders of the Sylow p-subgroups of certain finite general linear groups.

Lemma 2.8 *Let $q > 1$ be any prime-power and let p be any prime divisor of $q - 1$. Let p^e denote the full p-part of $q - 1$, and suppose that $p^e \geq 3$. Then for every positive integer m, the full p-part of $|\mathrm{GL}(m, q)|$ is p^{em+s} where p^s is the full p-part of $m!$.*

Let q be a prime-power and p a prime that satisfy the hypothesis of Lemma 2.8. For any integers k and m such that $1 \leq k < m$, the full p-part of $k!$ is less than or equal to the full p-part of $m!$, and so by Lemma 2.8, the full p-part of $|\mathrm{GL}(k, q)|$ is strictly smaller than the full p-part of $|\mathrm{GL}(m, q)|$. Hence a Sylow p-subgroup of $\mathrm{GL}(k, q)$ has smaller order than a Sylow p-subgroup of $\mathrm{GL}(m, q)$. We shall use this fact in the proof of Theorem A.

Proof of Theorem A By Theorem 2.3(i), the p-group W has a cyclic center and is therefore monolithic. Choose any prime-power $q > 1$ such that p^e is the full p-part of $q - 1$. Write $\Gamma = \mathrm{GL}(p^{n-1}, q)$ and let P be any Sylow p-subgroup of Γ. By the hypothesis $p^e \geq 3$ and by Theorem 1.1, we deduce that $P \cong W$. It follows that $\mathrm{mindeg}(W, q) \leq p^{n-1}$. For each positive integer k such that $k < p^{n-1}$, Lemma 2.8 implies that the p-part of the order of the general linear group $\mathrm{GL}(k, q)$ is strictly smaller than the p-power $|W|$, and so $\mathrm{GL}(k, q)$ contains no subgroup that is isomorphic to W. It follows that $\mathrm{mindeg}(W, q) = p^{n-1}$. Now Theorem 2.3(ii) implies that (W, q, p^{n-1}) is a monolithic triple. By Theorem 2.3(iii) and the fact that p^e is a divisor of $q-1$, (W, q, p^{n-1}) is indeed a good monolithic triple. Since W is isomorphic to

https://doi.org/10.4153/CMB-2011-088-3 Published online by Cambridge University Press

a Sylow p-subgroup of Γ, there is only one conjugacy class of subgroups of Γ whose members are isomorphic to W. Theorem 2.3(iv) yields $|\mathcal{F}(W,q)| = (p-1)p^{\beta(n)}$.

By Lemma 2.7, we may write $P = B \rtimes T$, where B is the group of all diagonal matrices of order dividing p^e in Γ, and where T is a transitive group of permutation matrices that is isomorphic to $W^1_{n-1}(p)$. Let S be the subgroup of Γ consisting of all permutation matrices, and note that $S \cong \mathrm{Sym}(p^{n-1})$. Theorem 2.5 yields $|\mathbf{N}_S(T):T| = (p-1)^{n-1}$. By Theorem 2.6, B is a characteristic subgroup of P. Since $P \cong W$, we have $|P| = p^{\alpha(n)}$. By Theorem 2.4, we obtain $|\mathbf{N}_\Gamma(P)| = (p-1)^{n-1}p^{\alpha(n)}(q-1)/p^e$. Now Theorem 2.2 yields

$$\begin{aligned}|\operatorname{Aut}(W)| &= [(p-1)p^{\beta(n)}][(p-1)^{n-1}p^{\alpha(n)-e}(q-1)]/(q-1)\\ &= (p-1)^n p^{\alpha(n)+\beta(n)-e},\end{aligned}$$

as desired to complete the proof. ■

3 Character Theory

In this section we determine useful character-theoretic information about the family of groups $W^e_n(p)$. First we introduce some notations. For an arbitrary finite group G, we write $\mathrm{Lin}(G)$ to denote the group of all linear ordinary characters of G. If ϵ is any primitive complex m-th root of unity for some positive integer m, we let $\mathbb{Z}(\epsilon)$ denote the subring of $\mathbb{C}$ that is generated by ϵ, and we mention that $\mathbb{Z}(\epsilon)$ is equal to the set of all $\mathbb{Z}$-linear combinations of complex m-th roots of unity. The following result includes Theorem 2.3.

Theorem 3.1 *Let p be a prime and let e and n be positive integers. Write $P = W^e_n(p)$. We define the set $\mathcal{F}_n = \{\chi \in \mathrm{Irr}(P) \mid \chi(1) = p^{n-1}$ and χ is faithful$\}$. Let ϵ be any primitive complex p^e-th root of unity. Then the following conditions hold.*

(i) *The center $\mathbf{Z}(P)$ is cyclic of order p^e.*
(ii) $|\mathrm{Lin}(P)| = p^{n+e-1}$.
(iii) *For each character $\mu \in \mathrm{Lin}(P)$, all the values of μ belong to the ring $\mathbb{Z}(\epsilon)$.*
(iv) *For each faithful character $\chi \in \mathrm{Irr}(P)$, we have $\chi(1) \geq p^{n-1}$.*
(v) *For each character $\chi \in \mathcal{F}_n$, all the values of χ belong to the ring $\mathbb{Z}(\epsilon)$.*
(vi) *If $n \geq 2$, then $|\mathcal{F}_n| = (p-1)p^{\beta(n)}$ where $\beta(n)$ is as defined in the Introduction.*

The following standard fact is used in our proof of Theorem 3.1.

Lemma 3.2 *Let G be a finite group having a unique minimal normal subgroup M. Let $1 < N \lhd G$ and let $\psi \in \mathrm{Irr}(N)$. Then the induced character ψ^G is faithful if and only if $M \nsubseteq \ker\psi$.*

Proof If $M \subseteq \ker\psi$, then [3, Lemma 5.11] yields $1 < M \subseteq \mathrm{core}_G(\ker\psi) = \ker\psi^G$, so ψ^G is not faithful. If $M \nsubseteq \ker\psi$, then using $\ker\psi^G \subseteq \ker\psi$ we obtain $M \nsubseteq \ker\psi^G$, and so by the uniqueness of M we have $\ker\psi^G = 1$, which says that ψ^G is faithful. ■

Proof of Theorem 3.1 Since p is fixed throughout this proof, we write $W^e_n = W^e_n(p)$ for arbitrary positive integers n and e. We proceed via induction on n. In the base case $n = 1$, it is clear that all conclusions hold. Henceforth let $n \geq 2$ and note that $P = N \rtimes \mathbb{Z}_p$, where N is a direct product of p copies of the group W^e_{n-1}. Each element of N is of the form $x = (x_1, \ldots, x_p)$ where $x_i \in W^e_{n-1}$ for $i \in \{1, \ldots, p\}$. Conjugation by an arbitrary element of P cyclically permutes the direct factors of N.

By the inductive hypothesis applied to part (i), the center $\mathbf{Z}(W^e_{n-1})$ is cyclic of order p^e. Let the element u be a generator for the cyclic group $\mathbf{Z}(W^e_{n-1})$. If $\mathbf{Z}(P) \nsubseteq N$, then using $|P{:}N| = p$ we obtain $P = \mathbf{Z}(P)N$, and so the permutation action of P on the p direct summands of N is trivial, contrary to what we know. Therefore $\mathbf{Z}(P) \subseteq N$.

It follows that $\mathbf{Z}(P) \subseteq \mathbf{Z}(N) = \langle u \rangle \times \cdots \times \langle u \rangle$. For an element $x \in \mathbf{Z}(N)$ to belong to $\mathbf{Z}(P)$, it is necessary and sufficient that x be invariant under conjugation by elements outside of N. But this happens if and only if the components of x are all equal to each other. Thus, for the element $z = (u, \ldots, u) \in N$ of order p^e, we have $\mathbf{Z}(P) = \langle z \rangle$, establishing part (i).

Since $N \lhd P$ and $|P{:}N| = p$, for each character $\psi \in \operatorname{Irr}(N)$, it is true that ψ extends to P in case ψ is P-invariant (by [3, Corollary 6.20]) and that ψ^P is irreducible in case ψ is not P-invariant. Each character $\psi \in \operatorname{Irr}(N)$ is of the form $\psi = \theta_1 \times \cdots \times \theta_p$ for $\theta_i \in \operatorname{Irr}(W^e_{n-1})$. We call $\theta_1, \ldots, \theta_p$ the components of ψ. For an arbitrary element $x = (x_1, \ldots, x_p) \in N$, we have $\psi(x) = \theta_1(x_1)\theta_2(x_2)\cdots\theta_p(x_p)$. We say that ψ is homogeneous in case $\theta_1 = \theta_2 = \cdots = \theta_p$. It is clear that ψ is P-invariant if and only if ψ is homogeneous.

The restriction of each linear character of P to the subgroup N is a linear P-invariant character of N and is therefore homogeneous. On the other hand, every homogenous linear character of N has p distinct extensions in $\operatorname{Lin}(P)$. Hence restriction to N defines a p-to-one mapping from the set $\operatorname{Lin}(P)$ onto the set of all homogenous linear characters of N. The number of homogenous linear characters of N is $|\operatorname{Lin}(W^e_{n-1})|$. It follows that $|\operatorname{Lin}(P)| = p \cdot |\operatorname{Lin}(W^e_{n-1})|$. The inductive hypothesis applied to part (ii) yields $|\operatorname{Lin}(W^e_{n-1})| = p^{(n-1)+e-1}$. We obtain $|\operatorname{Lin}(P)| = p^{n+e-1}$ as desired to establish part (ii).

It is clear that the group W^1_n is a homomorphic image of P. By [2, Satz III.15.3c], the elementary abelian p-group of rank n is a homomorphic image of W^1_n. Hence the elementary abelian p-group of rank n is a homomorphic image of P/P'. The abelian p-group $\operatorname{Lin}(P)$ is isomorphic to P/P', and therefore has rank at least n. Since $|\operatorname{Lin}(P)| = p^{n+e-1}$, it follows that the abelian p-group $\operatorname{Lin}(P)$ has exponent at most p^e, and so part (iii) is established.

We now argue that the element $z^{p^{e-1}}$ is contained in the kernel of every homogeneous character $\psi \in \operatorname{Irr}(N)$. Write $\psi = \theta \times \cdots \times \theta$ for some $\theta \in \operatorname{Irr}(W^e_{n-1})$. Because the element $u \in \mathbf{Z}(W^e_{n-1})$ has order p^e, we have $\theta(u) = \theta(1)\epsilon^m$ for some integer m. Hence $\theta(u^{p^{e-1}}) = \theta(1)\epsilon^{mp^{e-1}}$. Since $z = (u, \ldots, u)$, we have $z^{p^{e-1}} = (u^{p^{e-1}}, \ldots, u^{p^{e-1}})$. Recalling that ϵ is a primitive complex p^e-th root of unity, we obtain

$$\psi\big(z^{p^{e-1}}\big) = \prod_{i=1}^{p} \theta\big(u^{p^{e-1}}\big) = \prod_{i=1}^{p} \theta(1)\epsilon^{mp^{e-1}} = \theta(1)^p \epsilon^{mp^e} = \theta(1)^p = \psi(1),$$

which says that $z^{p^{e-1}} \in \ker \psi$, as claimed.

We now argue that for each faithful character $\chi \in \mathrm{Irr}(P)$ there exists $\psi \in \mathrm{Irr}(N)$ such that $\psi^P = \chi$ and $z^{p^{e-1}} \notin \ker \psi$. Let $\chi \in \mathrm{Irr}(P)$ be faithful. If the restriction χ_N is irreducible, then χ_N is P-invariant and therefore homogeneous, and so the preceding paragraph yields $z^{p^{e-1}} \in \ker \chi_N$, from which it follows that $z^{p^{e-1}} \in \ker \chi$, contradicting that χ is faithful. Hence χ_N is reducible. By [3, Corollary 6.19], we deduce that $\psi^P = \chi$ for some character $\psi \in \mathrm{Irr}(N)$. Since $\langle z^{p^{e-1}} \rangle$ is the unique minimal normal subgroup of P while ψ^P is faithful, Lemma 3.2 yields $z^{p^{e-1}} \notin \ker \psi$, as desired to establish our claim.

We define the set $\mathcal{S} = \{\psi \in \mathrm{Irr}(N) \mid z^{p^{e-1}} \notin \ker \psi \text{ and } \psi(1) = p^{n-2}\}$. We now argue that the rule $\psi \mapsto \psi^P$ defines a mapping from the set $\mathcal{S}$ to the set $\mathcal{F}_n$. Let $\psi \in \mathcal{S}$ be arbitrary. Because $z^{p^{e-1}} \notin \ker \psi$, we know that ψ is not homogeneous and therefore not P-invariant, and so ψ^P is irreducible. Since $z^{p^{e-1}} \notin \ker \psi$ while $\langle z^{p^{e-1}} \rangle$ is the unique minimal normal subgroup of P, Lemma 3.2 implies that ψ^P is faithful. Using $\psi(1) = p^{n-2}$ and $|P{:}N| = p$, we obtain $\psi^P(1) = p^{n-1}$. Hence $\psi^P \in \mathcal{F}_n$ and the mapping $\mathcal{S} \to \mathcal{F}_n$ is well defined. Next we argue that this mapping $\mathcal{S} \to \mathcal{F}_n$ is p-to-one and onto. Let $\chi \in \mathcal{F}_n$ be arbitrary. By the preceding paragraph, there exists $\psi \in \mathrm{Irr}(N)$ such that $\psi^P = \chi$ and $z^{p^{e-1}} \notin \ker \psi$. Since $\chi(1) = p^{n-1}$ and $\chi = \psi^P$ for $\psi \in \mathrm{Irr}(N)$ with $|P{:}N| = p$, we have $\psi(1) = p^{n-2}$. Therefore $\psi \in \mathcal{S}$ and the mapping is onto. Since $\psi \in \mathrm{Irr}(N)$ and ψ^P is irreducible, we know that ψ is not P-invariant. Each of the p distinct P-conjugates of ψ in $\mathrm{Irr}(N)$ also belongs to the set $\mathcal{S}$ and induces χ. Hence the mapping is p-to-one.

Since we have a p-to-one mapping from the set $\mathcal{S}$ onto the set $\mathcal{F}_n$, indeed $|\mathcal{F}_n| = |\mathcal{S}|/p$.

Case 1: Suppose $n = 2$. Thus N is a direct product of p copies of the cyclic group W_1^e of order p^e. Let $\chi \in \mathrm{Irr}(P)$ be faithful. Since P is a noncyclic p-group, we have $\chi(1) \geq p$, thereby establishing part (iv). By earlier observation, we know that $\chi = \psi^P$ for some $\psi \in \mathrm{Irr}(N)$. Hence χ vanishes off the normal subgroup N. We also know that $\chi_N = \psi_1 + \cdots + \psi_p$ for characters $\psi_1, \dots, \psi_p \in \mathrm{Irr}(N)$. Because N is homocyclic of exponent p^e, each of the values of each of the characters $\psi_1, \dots, \psi_p$ belongs to the ring $\mathbb{Z}(\epsilon)$. This establishes part (v).

Since $n = 2$, the condition $\psi(1) = p^{n-2}$ in the definition of $\mathcal{S}$ becomes $\psi(1) = 1$, which is true for every $\psi \in \mathrm{Irr}(N)$ since N is abelian. Thus

$$\mathcal{S} = \{\psi \in \mathrm{Irr}(N) \mid z^{p^{e-1}} \notin \ker \psi\}.$$

In order to calculate the cardinality $|\mathcal{S}|$, it suffices to count the linear characters of the abelian group N whose kernel does not contain the subgroup $\langle z^{p^{e-1}} \rangle$ of order p. The total number of linear characters of N is $|N| = p^{ep}$, and the number of these whose kernel contains $\langle z^{p^{e-1}} \rangle$ is $|N|/p = p^{ep-1}$. Hence $|\mathcal{S}| = p^{ep} - p^{ep-1} = (p-1)p^{ep-1}$. Therefore $|\mathcal{F}_2| = |\mathcal{S}|/p = (p-1)p^{ep-2}$. Since $\beta(2) = ep - 2$, we have established part (vi).

Case 2: Suppose $n > 2$. First we argue that the element $z^{p^{e-1}}$ is contained in the kernel of every character $\psi = \theta_1 \times \cdots \times \theta_p \in \mathrm{Irr}(N)$ having the property that none of the characters $\theta_1, \dots, \theta_p$ is faithful. First note that $\langle u^{p^{e-1}} \rangle$ is the unique minimal normal subgroup of W^e_{n-1}. Assuming that for each $i \in \{1,\ldots,p\}$ the character $\theta_i \in \mathrm{Irr}(W^e_{n-1})$ is not faithful, we have $u^{p^{e-1}} \in \ker\theta_p$ for each $i \in \{1,\ldots,p\}$. Using $z^{p^{e-1}} = (u^{p^{e-1}},\ldots,u^{p^{e-1}})$, we calculate that

$$\psi\big(z^{p^{e-1}}\big) = \prod_{i=1}^{p}\theta_i\big(u^{p^{e-1}}\big) = \prod_{i=1}^{p}\theta_i(1) = \psi(1),$$

which says that $z^{p^{e-1}} \in \ker\psi$, as claimed.

Let $\psi \in \mathrm{Irr}(N)$ be arbitrary and write $\psi = \theta_1 \times \cdots \times \theta_p$. Since $|P{:}N| = p$, the induced character ψ^P has degree $\psi^P(1) = p\psi(1)$ with $\psi(1) = \theta_1(1)\theta_2(1)\cdots\theta_p(1)$. Suppose that $z^{p^{e-1}} \notin \ker\psi$. By the preceding paragraph, there exists an index $k \in \{1,\ldots,p\}$ such that the character $\theta_k \in \mathrm{Irr}(W^e_{n-1})$ is faithful. The inductive hypothesis applied to part (iv) yields $\theta_k(1) \geq p^{n-2}$. It is clear that $\psi(1) \geq \theta_k(1)$, and so we obtain

$$\psi^P(1) = p\psi(1) \geq p\theta_k(1) \geq p\,p^{n-2} = p^{n-1}.$$

Note that $\psi \in \mathcal{S}$ if and only if $\psi(1) = p^{n-2}$. By the preceding chain of inequalities, the condition $\psi(1) = p^{n-2}$ occurs if and only if $\theta_k(1) = p^{n-2}$ while $\theta_i(1) = 1$ for each $i \in \{1,\ldots,p\}$ such that $i \neq k$.

For each faithful character $\chi \in \mathrm{Irr}(P)$, we proved earlier that there exists $\psi \in \mathrm{Irr}(N)$ such that $\psi^P = \chi$ and $z^{p^{e-1}} \notin \ker\psi$, and so the preceding paragraph yields $\chi(1) = \psi^P(1) \geq p^{n-1}$, thereby establishing part (iv).

The preceding observations give us the following more explicit characterization of the members of the set $\mathcal{S}$. For each character $\psi = \theta_1 \times \cdots \times \theta_p \in \mathrm{Irr}(N)$, it is true that $\psi \in \mathcal{S}$ if and only if exactly one of the characters $\theta_1,\ldots,\theta_p$ belongs to the set $\mathcal{F}_{n-1}$ (and is hence nonlinear because W^e_{n-1} is noncyclic for $n > 2$), while the remaining $p-1$ such characters are linear.

We now argue that every value of each character belonging to the set $\mathcal{S}$ lies in the ring $\mathbb{Z}(\epsilon)$. Let $\psi = \theta_1 \times \cdots \times \theta_p \in \mathcal{S}$ be arbitrary. By the preceding paragraph, there exists a unique index $k \in \{1,\ldots,p\}$ such that $\theta_k \in \mathcal{F}_{n-1}$ while $\theta_i \in \mathrm{Lin}(W^e_{n-1})$ for each $i \in \{1,\ldots,p\}$ such that $i \neq k$. By the inductive hypothesis applied to part (iii) and part (v), every value of each of the characters $\theta_1,\ldots,\theta_p$ lies in the ring $\mathbb{Z}(\epsilon)$. Thus for an arbitrary element $x = (x_1,\ldots,x_p) \in N$ we have $\psi(x) = \theta_1(x_1)\theta_2(x_2)\cdots\theta_p(x_p) \in \mathbb{Z}(\epsilon)$.

We now establish part (v). Let $\chi \in \mathcal{F}_n$ be arbitrary. Thus $\chi = \psi^P$ for some character $\psi \in \mathcal{S}$. Since $\psi \in \mathrm{Irr}(N)$, the character χ vanishes off the normal subgroup N. The restriction χ_N is a sum of p characters belonging to the set $\mathcal{S}$. By the preceding paragraph, it follows that every value of χ_N lies in the ring $\mathbb{Z}(\epsilon)$, as required to establish part (v).

It remains to establish part (vi). First we use our characterization of the set $\mathcal{S}$ to determine the cardinality of the set $\mathcal{S}$. To construct an arbitrary member ψ of the set $\mathcal{S}$, we begin by choosing some character in $\mathcal{F}_{n-1}$. Next we decide in which of the p components of ψ this character chosen from $\mathcal{F}_{n-1}$ will appear. We then fill each of the remaining $p-1$ components of ψ with an arbitrary member of $\mathrm{Lin}(W^e_{n-1})$. By counting the total number of ways to carry out this process, we obtain

$$|\mathcal{S}| = |\mathcal{F}_{n-1}| \cdot p \cdot |\mathrm{Lin}(W^e_{n-1})|^{p-1}.$$

https://doi.org/10.4153/CMB-2011-088-3 Published online by Cambridge University Press

The inductive hypothesis applied to part (ii) yields $|\mathrm{Lin}(W_{n-1}^{e})| = p^{n+e-2}$. Using $|\mathcal{F}_n| = |\mathcal{S}|/p$, we deduce that $|\mathcal{F}_n| = |\mathcal{F}_{n-1}| \cdot p^{(p-1)(n+e-2)}$. Since $n > 2$, the inductive hypothesis applied to part (vi) yields $|\mathcal{F}_{n-1}| = (p-1)p^{\beta(n-1)}$. It follows that

$$|\mathcal{F}_n| = (p-1)p^{\beta(n-1)}p^{(p-1)(n+e-2)}.$$

It is straightforward to verify that $\beta(n-1) + (p-1)(n+e-2) = \beta(n)$. Hence we conclude that indeed $|\mathcal{F}_n| = (p-1)p^{\beta(n)}$, as required to establish part (vi). ■

Acknowledgements We thank the referee for suggesting improvements to the proof of Theorem 3.1.

References

[1] J. L. Alperin and P. Fong, *Weights for symmetric and general linear groups.* J. Algebra **131**(1990), no. 1, 2–22. http://dx.doi.org/10.1016/0021-8693(90)90163-I
[2] B. Huppert, *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften 134. Springer-Verlag, Berlin, 1967.
[3] I. M. Isaacs, *Character Theory of Finite Groups*. Dover, New York, 1994.
[4] P. Lentoudis, *Détermination du groupe des automorphismes du p-groupe de Sylow du groupe symétrique de degré p^m: l'idée de la méthode.* C. R. Math. Rep. Acad. Sci. Canada **7**(1985), no. 1, 67–71.
[5] ———, *Le groupe des automorphismes du p-groupe de Sylow du groupe symétrique de degré p^m: résultats.* C. R. Math. Rep. Acad. Sci. Canada **7**(1985), no. 2, 133–136.
[6] J. M. Riedl, *The number of automorphisms of a monolithic finite group.* J. Algebra **322**(2009), no. 12, 4483–4497. http://dx.doi.org/10.1016/j.jalgebra.2009.07.034

Department of Theoretical and Applied Mathematics, University of Akron, Akron, OH 44325-4002, USA
e-mail: riedl@uakron.edu